

IN THE UNITED STATES DISTRICT COURT
FOR NORTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF
ONE (1) ALCATEL MODEL A405DL,
CELLULAR PHONE, IMEI#
015400002184013

Case No. 1:19-mj-113

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

Your affiant, Trooper John W. Smith, a member of the West Virginia State Police, being duly sworn according to law does depose:

1. Your affiant has been a member of the West Virginia State Police for nineteen years. Before serving as a State Trooper, your affiant was a member of the Clarksburg Police Department for five years, during which time your affiant was assigned to the Harrison-Lewis-Upshur Counties Narcotics Task Force for approximately three years, specifically for the purpose of investigating criminal violations concerning controlled substances. Since November 2005, your affiant has been assigned to the West Virginia State Police Bureau of Criminal Investigations, which is primarily responsible for investigating controlled substance violations and organized crime against the State of West Virginia and the United States of America. During his law enforcement career, your affiant has been personally involved with more than a thousand criminal investigations involving crimes against the state and federal government. Your affiant also has received extensive training concerning narcotics investigation and interdiction.

2. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of your affiant's knowledge about this matter.

BACKGROUND

3. Dismas Charities is one of the largest, not-for-profit providers of residential re-entry services in the United States. The Dismas Charities of Clarksburg houses federal inmates in preparation for re-entry into society. The facility itself is locked and all entry to the facility is controlled. Each inmate is required to register any cellular phones that they have in their possession and are only allowed to have one cellular phone and not permitted social media. Each cellular phone is required to be turned in every night at the facility.

4. Based on the criminal history, Mario Grisom was arrested on July 7, 2015 on a federal charge of Sexual Exploitation of a Minor. The disposition section listed a guilty plea entered on **March 16, 2017** to a charge for **Sex Trafficking of a Child** in violation of 18 U.S.C. §1591, a **60** month sentence of imprisonment, five years supervised release, cooperation in DNA collection, and sex offender registration and notification requirements.

5. On July 5, 2019, Juanita Schoonover the Director of the Dismas Charities located in Harrison County, West Virginia, Northern District of West Virginia, reported to your affiant that Mario Grisom, a resident of said facility, had been found to be in possession of a bag containing a substance with crystal and powder like appearance, consistent with crystal methamphetamine, during a search when entering the Dismas Charities facility. Mario Grisom was subsequently observed attempting to communicate on a cellular smartphone, attempted to hide the phone at his side while sitting within the entry to the facility, and refused to divulge the passcode to the smartphone when confronted by Dismas Charities employees.

6. Federal Bureau of Prisons website, list Mario Grisom as a current Bureau of Prisons inmate (Register #16788-042, Baltimore RRM, listing a release date of 11/11/2019).

7. The requested warrant seeks authority to search an Alcatel Model A405DL, cellular phone, IMEI# 015400002184013, that was seized from Mario Grisom on July 5, 2019, by Dismas Charities employees, hereafter referred to as the "SUBJECT DEVICE" (described in attachment A and incorporated herein by reference), which is currently in law enforcement possession and the extraction from that property of electronically stored information as described in Attachment B (incorporated herein by reference).

PROBABLE CAUSE

8. On July 5, 2019, Juanita Schoonover, Director Dismas Charities, reported to your affiant that Mario Grisom, a resident of the facility, had been searched upon reentering and was found to possess a bag containing a substance with crystal and powder like appearance consistent with crystal methamphetamine. Mario Grisom was subsequently observed attempting to communicate on an unregistered cellular smartphone and attempted to hide it at his side while sitting within the entry to the facility. When confronted by Dismas Charities employees, Grisom refused to divulge the passcode to the smartphone he possessed in violation of the rules of Dismas Charities. Employees then seized the bag with the crystal-like powder and the smartphone, an Alcatel Model A405DL, cellular phone, IMEI# 015400002184013.

9. Your affiant took possession of the bag of substance and the Alcatel Model A405DL, cellular phone, IMEI# 015400002184013 (SUBJECT DEVICE). The SUBJECT DEVICE is currently stored at the Greater Harrison County Drug and Violent Crime Task Force office in Harrison County, West Virginia.

10. On Monday, July 8, 2019, Brian Purkey Commander of the Greater Harrison County Drug and Violent Crime Task Force (TF), and your affiant conducted a presumptive test of a sample taken from the bag previously found to be in possession of by Mario Grisom. The

NARK II Narcotics Analysis Reagent Kit was utilized for the presumptive test of Methamphetamine and MDMA (Ecstasy). The presumptive test provided a positive result.

11. On Tuesday, July 9, 2019, TF/Commander Brian Purkey and your affiant interviewed Gail Rowell, a friend of Mario Grisom. Ms. Rowell had been a friend of Grisom for approximately one month. During the interview, Gail Rowell advised that another friend, Robert Tricase, had previously provided her with a black bag containing salts to be used for good luck. Ms. Rowell advised she kept within the bag of salts in her vehicle for good luck. On Friday, July 5, 2019, Ms. Rowell provided a ride to Grisom in her vehicle. Ms. Rowell advised that the bag of salts must have fallen into the shoes of Mario Grisom prior to dropping him off at the Dismas Charities. Gail Rowell advised she never looked within the bag personally, so she could not advise what the substance looked like that was contained within the bag. She could merely say that her friend told her the bag only contained salts. Gail Rowell advised the bag must have fallen into the shoe of Mario Grisom, but was unable to provide an explanation on how that was possible without the knowledge of Mario Grisom given the size of the bag.

12. Your affiant conducted a field test of Pink Himalayan Salt purchased from a local grocery store, utilizing the NARK II Narcotics Analysis Reagent Kit utilized for the presumptive test of Methamphetamine and MDMA (Ecstasy). The presumptive test also provided a positive result of the Pink Himalayan Salt.

13. On Thursday, July 11, 2019, Gail Rowell allowed your affiant to search her personal cellular phone and review the communications and content within her phone. Gail Rowell explained to your affiant that Mario Grisom had three different cellular phones she used to contact him. Ms. Rowell advised all three phone numbers for Grisom were saved within her contacts under "RIO" (412-512-9196), "RIO2" (304-517-4895) and "RIO3" (681-622-0391).

14. Your affiant reviewed the content of Ms. Rowell's cellular phone, and the phone revealed communication occurred between Gail Rowell Mario Grisom on all three of Grisom's phone numbers.

15. On Thursday, July 11, 2019, Juanita Schoonover, Director Dismas Charities, informed your affiant that employees took possession of two additional cellular phones that were found to be in possession of Mario Grisom. Your affiant took possession of the two additional cellular phones, that being an Sprint Coolpad Model 3310A, SN# 331XF18CS0004929, and an Alcatel Model 4044O cellular phone, IMEI# 015411001145293, and they are currently stored at the Greater Harrison County Drug and Violent Crime Task Force office in Harrison County, West Virginia.

16. Your affiant reviewed the Sex Offender Registration File contained at the West Virginia State Police Bridgeport Detachment for Mario Grisom. Your affiant learned that on May 10, 2019, Mario Grisom reported to the West Virginia State Police as required for his sex offender registration requirements. Mario Grisom completed the "Notification of Sex Offender Responsibility and Registration Certification," that provides a list of Grisom's responsibilities. The form explained that Grisom is required to register any change in registration information, including, but not limited to, the following: physical and mailing address, vehicle, internet, phone, screen names, and e-mail accounts. The records revealed that Mario Grisom provided one cellular phone number (412-516-9196) to the West Virginia State Police on May 10, 2019. On June 5, 2019, Mario Grisom updated his sex offender registration information with the West Virginia State Police, and provided an employer, "Meaghers Irish Pub," but no additional phones were provided by Mario Grisom.

17. On July 12, 2019, your affiant learned from Dismas Charities that Mario Grisom reported to staff that he was also employed at the Hilton Garden Inn beginning on May 30, 2019. This additional employment was not reflected in the June 5, 2019, West Virginia State Police registration form.

18. Your affiant reviewed the criminal history for Mario Grisom and noted the following arrests: **7/7/2015**-Sexual Exploitation of Minor (18 U.S.C. 1591), **10/21/1997**-Robbery and Conspiracy, **08/13/1999**-Simple Assault, **8-28-1999**-Receiving Stolen Property, **4-28-2001**-Receiving stolen property, Drug/Dev and Cosmetic Act and Theft by Unlawful taking or Disp, **5/14/2001**-Simple Assault, **10-09-2001**-Unsworn Falsification to Auth and False Report to Law Enforcement and Corruption of Minors. **1/18/2002**-Loit and Prowling at Night Time, Resisting Arrest, Escape, Vio CS Drug/Dev and Cosmetic Act and Disorderly Conduct, **3/15/2002**- DUI of Alcohol or Controlled substance, Driving while susp or revoked, DRV required to be Licensed, **10/3/2002**-Vio CS/Drug/Dev and Cosmetic Act, **10/14/2002**- Vio CS/Drug/Dev and Cosmetic Act, **10/4/2004**- Vio CS/Drug/Dev and Cosmetic Act, **1/2/2005**-Receiving Stolen Property, CS/Drug/Dev and Cosmetic Act, **5/2/2006**- Vio CS/Drug/Dev and Cosmetic Act, **9/14/2006**-Forgery, Unsworn Falsification to Auth and Viol of Elec and Elel Dist Code, **12/20/2006**- Vio CS/Drug/Dev and Cosmetic Act and DRV Required to be Licensed, **2/1/2008**- DRV while susp-Revoked, DUI of Alcohol or Controlled Substance, **10/28/2008**-Driving while Susp or Revoked and Vio CS/Drug/Dev and Cosmetic Act, **11/20/2009**- DRV Required to be Licensed, VIO CS/Drug/Dev and Cosmetic Act, **12/06/2009**-Vio CS/Drug /Dev and Cosmetic Act, Driving while Susp or Revoked, **9/14/2010**-Altered/Frg/CTFT Doc and Plates, DRV While Susp-Revoked, **4/08/2011**-Vio CS/Drug/Dev and Cosmetic Act, **9/26/2013**-Robbery, **2/4/2014** – Theft by Unlawful Taking or Disp, Receiving Stolen Property, Open Lewdness, Vio CS/Drug/DEV and

Cosmetic Act, 5/1/2015-Prostitution and Related Offense, Possessing instrument of Crime, Driving While Susp or Revoked and Criminal Conspiracy.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. As described in Attachment B, this application seeks permission to search for information that might be found within the SUBJECT DEVICE. Based on my knowledge, training, and experience, as well as information relayed to me by agents and others involved in this investigation and in the forensic examination of digital devices, your affiant respectfully submits that there is probable cause to believe that the records and information described in Attachment B will be stored in the SUBJECT DEVICE for at least the following reasons:

- a. Based on my knowledge and experience, your affiant knows that persons who traffic and distribute controlled substances frequently rely on cellular phones, such as the SUBJECT DEVICE, to facilitate their drug trafficking enterprises by staying in regular communication with their sources of supply, money and drug couriers, and clientele, based locally and far away, and that drug dealers utilize communication devices to receive and send information relating to drug activities through the use of cellular calls, e-mails and other communication means. Drug traffickers will utilize digital devices, like the SUBJECT DEVICE, to access websites to facilitate illegal activity and to communicate with co-conspirators online or via peer-to-peer communication sites; to store documents and records relating to their illegal activity, which can include logs of online "chats" with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for

instant messaging and social medial accounts; financial and personal identification data, including bank account numbers, and credit card numbers relating to proceeds from the illegal sale of controlled substances; and records of illegal drug transactions, including the accounting of illegal proceeds for purposes of splitting those proceeds with co-conspirators and track money due for past sales of controlled substances. Furthermore, your affiant knows that drug traffickers utilize cellular phones, such as the SUBJECT DEVICE to photograph and/or video themselves with large amounts of United States currency, firearms, and/or and controlled substances to utilize the photographs on peer-to-peer communication sites to further their reputation and build their clientele. Additionally, your affiant knows that drug traffickers will utilize their cellular devices as ledgers to track money owed and/or proceeds from the sales of controlled substances, as well as access bank records to track proceeds from the sales of controlled substances.

- b. Drug traffickers and their associates frequently carry and use multiple (and sometimes numerous) cell phones. They use different phones to facilitate and protect their unlawful business, often by designating separate phones for specific buyers and suppliers.
- c. Individuals who engage in trafficking and distribution of controlled substances, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

- d. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device, such the SUBJECT DEVICE, or a micro SD card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s storage capacity, smart phone, or other digital device habits.

20. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the SUBJECT DEVICE were used, the purpose of its use, who used it (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, your affiant respectfully submits there is probable cause to believe that the records and information described in Attachment B will be stored in the SUBJECT DEVICE for at least the following reasons:

- a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as pictures, videos, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the SUBJECT DEVICE are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, memory card, or other electronic storage media image as a whole. Digital data stored in the SUBJECT DEVICE, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file. Virtual memory paging systems can leave digital data on a hard drive that show what tasks and

processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive of the device or memory card that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, and the times a smart phone or other digital device was in use. Smart phone and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

- b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

21. I know that when an individual uses a digital device to traffic or distribute controlled substances, the individual’s device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device

is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense and the identities of those perpetrating it.

22. Based upon the forgoing facts, your affiant believes there is sufficient probable cause for the issuance of a Search Warrant to examine and image the devices listed in the Property to Be Searched Attachment to seek evidence related to violations of 21 U.S.C. § 846 – Conspiracy to Distribute a Controlled Substances, and 21 U.S.C. § 841 – Distribution of and Possession with the Intent to Distribute Controlled Substance. Your affiant respectfully requests the issuance of a search warrant for the SUBJECT DEVICE, particularly described in Attachment A, in order to search for and seize the electronic evidence.

23. The anticipated forensic examination of the device may take longer than fourteen days, and such examination may take place outside the district. Devices such as the SUBJECT DEVICE will continue to hold the electronically stored information desired indefinitely.

24. In my training and experience, I know that the SUBJECT DEVICE have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE first came into the possession law enforcement.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant, your affiant is applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ

techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, your affiant submits there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

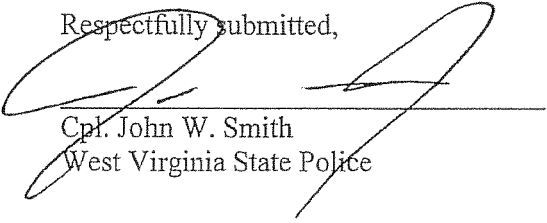
27. The seizure and subsequent forensic analysis of the listed cellular phones listed in Attachment A are communication devices designed for use on any cellular and / or other wireless networks, otherwise known as smartphones, cellular telephones, and tablet computers. Also included is any digital and / or electronic device(s) contained within any of the digital device items described in this application and search warrant. These items may include any and all SIM cards (Subscriber Identity Modules), digital media cards, embedded memory chips contained within the digital devices, or other digital storage media used with the above described electronic devices. It should be further noted and explained that any forensic analysis of mobile devices, especially those that are secured with a password, passcode, gesture, or biometrics are especially at risk for damage and will possibly be returned non-operational depending on the methods used to gain access to the data.

CONCLUSION

28. Based upon the forgoing facts, I believe there is sufficient probable cause for the issuance of a Search Warrant for the property listed in Attachment A, to seek evidence related to violations of Title 21, United States Code, Sections 846 and 841(a)(1).

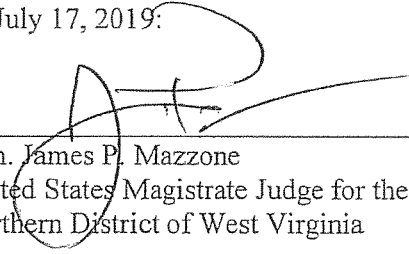
29. The applied-for warrant would authorize the imaging, examination and analysis of the SUBJECT DEVICE for the purpose of identifying electronically stored data, particularly described in Attachment B.

Respectfully submitted,



Cpl. John W. Smith
West Virginia State Police

Subscribed and sworn to before me
on July 17, 2019:



Hon. James P. Mazzone
United States Magistrate Judge for the
Northern District of West Virginia